



Examples

FortiManager 7.4.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



May 15, 2023

FortiManager 7.4.0 Examples

02-740-909880-20230515

TABLE OF CONTENTS

Change Log	4
Introduction	5
Device Manager	6
Exporting a policy package from one FortiManager to another	6
VPN Manager	8
Configuring a full mesh VPN topology within a VPN console	8
System Settings	14
Configuring and debugging FortiManager HA clusters	14
Configuring the primary FortiManager unit in an HA cluster	14
Configuring backup FortiManager units in an HA cluster	15
Generating and downloading HA debug logs	15
Creating administrator accounts with restricted access	16
Restricting administrator access to ADOMs	16
Restricting administrator access to device groups	18
Restricting administrator access to policy packages	19
Others	21
Managing FortiAnalyzer from FortiManager	21
Adding FortiAnalyzer to FortiManager	21
Viewing managed FortiAnalyzer behavior	25
Centrally configuring FortiGate to send logs to managed FortiAnalyzer	26
Viewing logs and reports for managed FortiAnalyzer units	26
Managing multiple FortiAnalyzer units	27
Troubleshooting managed FortiAnalyzer units	28
Creating a third party blocklist provider workflow	29

Change Log

Date	Change Description
2023-05-15	Initial release.

Introduction

This document serves as a reference guide to common FortiManager 7.4 configuration and deployment scenarios. The scope of this document is to explain specific examples and include information required for those examples to work. The examples rely on the other documents to provide full product information.



For further FortiManager information, refer to the [FortiManager Administration Guides](#) available on the [Fortinet Docs Library](#).

This section includes configuration examples for FortiManager 7.4:

- [Device Manager on page 6](#)
- [VPN Manager on page 8](#)
- [System Settings on page 14](#)
- [Others on page 21](#)

Device Manager

This section contains the following topics:

- [Exporting a policy package from one FortiManager to another](#) on page 6

Exporting a policy package from one FortiManager to another

In this example, you will learn how to export a policy package from one FortiManager to another FortiManager.

To export a policy package from one FortiManager to another FortiManager:

1. Select a FortiManager policy package and installation target you want to export:
 - a. Select a FortiManager policy package and its installation target.
For example,
Policy Package: PP_001
Installation Target: Device1
2. Download the latest revision:
 - a. Go to *Device Manager > Device & Groups >* and double-click the installation target device (Device1 in this example).
 - b. Go to *Dashboard > Configuration and Installation > Total Revisions*.
 - c. Download the latest revision (for example, Revision 1).
3. Add the device to the second FortiManager:
 - a. Go to your second FortiManager.
 - b. Go to *Device Manager > Device & Groups >* and click *Add Device*. The Add Device wizard displays.
Its SN must be similar to the one you got the revision from. It can be the same as the original SN, or you can take the SN prefix (the first six characters) and append 10 digits to it.
For example, FG200D12345985242 is the original SN.
Prefix: FG200D
Appended 10 Digits: 0000000001
The new SN will be: FG200D0000000001.
 - c. Select *Add Model Device* and complete the wizard.
4. Import the revision to the second FortiManager:
 - a. On your second FortiManager device, go to *Device Manager > Device & Groups* and double-click the model device. The Device Dashboard displays.
 - b. Go to *Dashboard > Configuration and Installation > Total Revisions*.
 - c. Right-click the empty revision list and select *Import Revision > Revision 1*.
 - d. Go to *Device Manager > Device & Groups*.
 - e. Right-click your model device and select *Import Policy*. The wizard displays.

- f. Complete the wizard.
- g. Go to *Policy & Objects*. The policy package and its used objects are displayed.



For further FortiManager information, refer to the [FortiManager Administration Guides](#) available on the [Fortinet Document Library](#).

VPN Manager

This section contains the following topics:

- [Configuring a full mesh VPN topology within a VPN console on page 8](#)

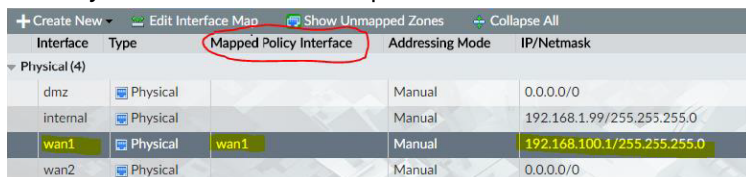
Configuring a full mesh VPN topology within a VPN console

This is an example on how to configure a simple full mesh VPN with:

- Three FortiGate (FGT) devices
- A pre-shared key for authentication
- An auto-up tunnel setting
- Static routes

To configure a full mesh VPN topology within a VPN console:

1. Add FortiGate devices and map all interfaces:
 - a. Go to *Device Manager*. Add three FortiGate devices by clicking *Add Device*. Follow the wizard to add each device.
 - b. Go to *Policy & Objects > Policy Packages* and define the *Zone* interfaces.
 - c. Go to *Device Manager* and select a device.
 - d. Go to *System > Interface* and map the interfaces to the *Zone* interfaces.



Interface	Type	Mapped Policy Interface	Addressing Mode	IP/Netmask
Physical (4)				
dmz	Physical		Manual	0.0.0.0/0
internal	Physical		Manual	192.168.1.99/255.255.255.0
wan1	Physical	wan1	Manual	192.168.100.1/255.255.255.0
wan2	Physical		Manual	0.0.0.0/0

2. Create firewall addresses for protected subnets:
 - a. Go to *Policy & Objects > Firewall Objects > Address* to manage the firewall addresses.
 - b. VPNs only support firewall addresses with the type set to *subnet (IP/Netmask)*. The firewall addresses will be used as protected subnets to generate static routes among the FortiGate devices.
3. Create a VPN community:
 - a. Go to *VPN Manager > IPsec VPN Communities > Create New*.
 - b. Set the *VPN Topology* type to *Site to Site*.
 - c. Define the *Authentication* method with a *Pre-shared Key*.

d. Specify the encryption and hash methods.

VPN Topology Setup Wizard

Authentication & Encryption Settings:

Authentication: Certificates **Pre-shared Key**

☐ Generate(random)
☒ Specify

Encryption

IKE Security (Phase 1) Properties

1-Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA-1"/>	+
2-Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="MD5"/>	+

IPsec Security (Phase 2) Properties

1-Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA-1"/>	+
2-Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="MD5"/>	+

< Back Next > Cancel

e. After defining the authentication methods and encryption properties, click *Next*.**f. Configure the *VPN Phase 1* and *Phase 2* settings.**

VPN Topology Setup Wizard

VPN Zone: ON

☒ Create Default Zones
☐ Use Custom Zone

IKE Security Phase 1 Advanced Properties

Diffie Hellman Group(s): ☐ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17
☐ 18 ☐ 19 ☐ 20 ☐ 21

Exchange Mode: ☐ Aggressive ☒ Main(ID Protection)

Key Life: (120-172800 seconds)

Dead Peer Detection: ON

IPsec Security Phase 2 Advanced Properties

Diffie Hellman Group(s): ☐ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17
☐ 18 ☐ 19 ☐ 20 ☐ 21

Replay Detection: ON

Perfect Forward: ON

< Back Next > Cancel

- g. For the *IPSec Phase 2* setting, set the tunnel to *Auto-Negotiate*.

VPN Topology Setup Wizard

IPsec Security Phase 2 Advanced Properties

Diffie Hellman Group(s) ☐ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17
☐ 18 ☐ 19 ☐ 20 ☐ 21

Replay Detection ☒ ON

Perfect Forward Secrecy(PFS) ☒ ON

Key Life ☒ Seconds ☐ KB ☐ Both
 1800 seconds 5120 KB

Autokey Keep Alive ☒ ON

Auto-Negotiate ☐ OFF

NAT-traversal ☒ Enable ☐ Disable ☐ Forced

Keep Alive Frequency 10 (10-900 seconds)

Advanced Options >

< Back Next > Cancel

VPN configuration summary:

Name Full

Description test full mesh

Topology ☒ Full Meshed

Authentication Certificates Pre-shared Key
☐ Generate(random)
☒ Specify

Encryption

IKE Security (Phase 1) Properties

1-Encryption	DES	Authentication	SHA-1	+ -
2-Encryption	DES	Authentication	MD5	+ -

IPsec Security (Phase 2) Properties

1-Encryption	DES	Authentication	SHA-1	+ -
2-Encryption	DES	Authentication	MD5	+ -

VPN Zone ☒ ON
☒ Create Default Zones
☐ Use Custom Zone

IKE Security Phase 1 Advanced Properties

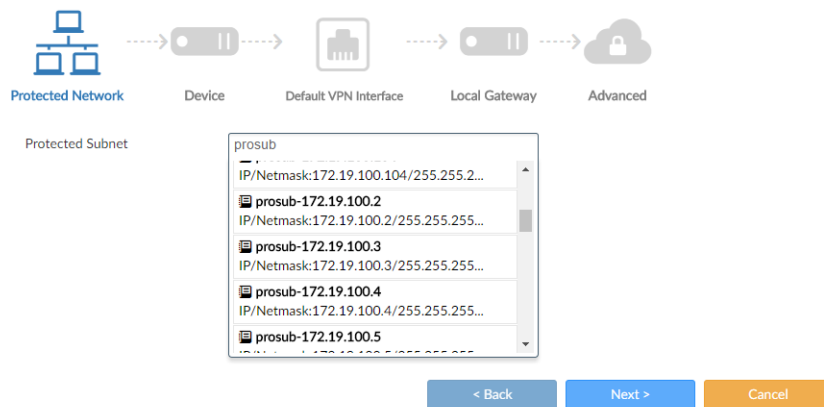
Diffie Hellman Group(s) ☒ 2 ☒ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17
☐ 18 ☐ 19 ☐ 20 ☐ 21

4. Add a VPN gateway:

- Go to *VPN Manager > IPsec VPN Communities* and select your VPN community.
- Right-click the community and select *Add Managed Gateway*.

- c. Add a *Protected Network*. There can be more than one protected networks.

VPN Gateway Setup Wizard - ☒ Full



The screenshot shows the 'Protected Network' step of the VPN Gateway Setup Wizard. The wizard is titled 'VPN Gateway Setup Wizard - ☒ Full'. The progress bar indicates the current step is 'Protected Network'. The wizard consists of five steps: Protected Network, Device, Default VPN Interface, Local Gateway, and Advanced. The 'Protected Network' step is active, showing a list of protected subnets. The list includes 'prosub' and several subnets with IP/Netmask addresses: 'prosub-172.19.100.2', 'prosub-172.19.100.3', 'prosub-172.19.100.4', and 'prosub-172.19.100.5'. The 'Device' step is highlighted in blue. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

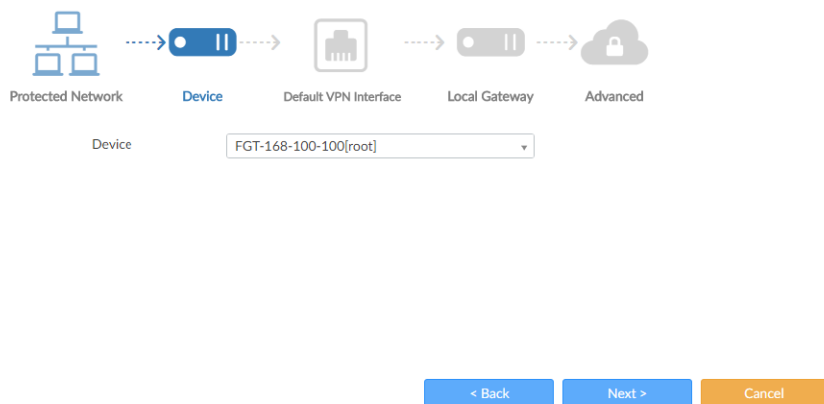
Protected Subnet

Protected Subnet
prosub
IP/Netmask:172.19.100.104/255.255.2...
prosub-172.19.100.2
IP/Netmask:172.19.100.2/255.255.255...
prosub-172.19.100.3
IP/Netmask:172.19.100.3/255.255.255...
prosub-172.19.100.4
IP/Netmask:172.19.100.4/255.255.255...
prosub-172.19.100.5

< Back Next > Cancel

- d. Select a *Device*.

VPN Gateway Setup Wizard - ☒ Full



The screenshot shows the 'Device' step of the VPN Gateway Setup Wizard. The wizard is titled 'VPN Gateway Setup Wizard - ☒ Full'. The progress bar indicates the current step is 'Device'. The wizard consists of five steps: Protected Network, Device, Default VPN Interface, Local Gateway, and Advanced. The 'Device' step is active, showing a dropdown menu for selecting a device. The dropdown menu is open, showing the selected device 'FGT-168-100-100[root]'. The 'Device' step is highlighted in blue. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.






Device

FGT-168-100-100[root]

< Back Next > Cancel

- e. Select a *Default VPN Interface*. The default VPN interface should have a valid IP and be mapped.

VPN Gateway Setup Wizard - ☒ Full






    

Protected Network Device **Default VPN Interface** Local Gateway Advanced

Default VPN Interface

- i. Optionally, specify the *Local Gateway*. This option can be left blank in most cases.

VPN Gateway Setup Wizard - ☒ Full

Protected Network Device Default VPN Interface **Local Gateway** Advanced

Local Gateway

- f. Go to *Routing* and select *Automatic* to generate static routes.

VPN Gateway Setup Wizard - ☒ Full

Routing

☐ Manual (via Device Manager)
☒ Automatic

Local ID

Advanced Options ▾

authpasswd

authusr

banner

dns-mode

domain

public-ip

route-overlap

- i. If *Manual* is selected, go to the *Device Manager* to set the IP on the relevant IPSec interfaces and define the routings manually.

VPN gateway configuration settings summary:

Edit Gateway

Protected Subnet	prosub-172.19.100.1
Device	FGT-168-100-1[root]
Default VPN Interface	wan1
Local Gateway	IP Address
Routing	<input type="radio"/> Manual (via Device Manager) <input checked="" type="radio"/> Automatic
Local ID	
Advanced Options >	

5. Create firewall policies:

- a. Go to *Policy & Objects > Policy Package* to create policies among the default VPN zones and protected-subnet interfaces.
- b. Use the *Install On* option to restrict policies applied on specific FortiGate devices.

Seq#	From	To	Source	Destination	Schedule	Service	Action	Log	NAT	Install On
1	loop1	vpnmgmt_full_rm	all	all	always	ALL	Accept	Log Security Ev	Disabled	<input checked="" type="checkbox"/> FGT-168-100-4 (root) <input checked="" type="checkbox"/> FGT-168-100-2 (root) <input checked="" type="checkbox"/> FGT-168-100-3 (root) <input checked="" type="checkbox"/> FGT-168-100-1 (root) <input checked="" type="checkbox"/> FGT-168-100-5 (root)
2	vpnmgmt_full_rm	loop1	all	all	always	ALL	Accept	Log Security Ev	Disabled	<input checked="" type="checkbox"/> FGT-168-100-4 (root) <input checked="" type="checkbox"/> FGT-168-100-2 (root) <input checked="" type="checkbox"/> FGT-168-100-3 (root) <input checked="" type="checkbox"/> FGT-168-100-1 (root) <input checked="" type="checkbox"/> FGT-168-100-5 (root)
3	loop1	vpnmgmt_full_sp	prosub-172.19.100.22 prosub-172.19.100.23 prosub-172.19.100.24 prosub-172.19.100.25 prosub-172.19.100.26 prosub-172.19.100.27 prosub-172.19.100.28 prosub-172.19.100.29 prosub-172.19.100.30	all	always	ALL	Accept	Log All Sessions	Disabled	<input checked="" type="checkbox"/> FGT-168-100-22 (root) <input checked="" type="checkbox"/> FGT-168-100-23 (root) <input checked="" type="checkbox"/> FGT-168-100-24 (root) <input checked="" type="checkbox"/> FGT-168-100-25 (root) <input checked="" type="checkbox"/> FGT-168-100-26 (root) <input checked="" type="checkbox"/> FGT-168-100-27 (root) <input checked="" type="checkbox"/> FGT-168-100-28 (root) <input checked="" type="checkbox"/> FGT-168-100-29 (root) <input checked="" type="checkbox"/> FGT-168-100-30 (root)

- c. Remember to create policies for bi-directional traffic.



For further FortiManager information, refer to the [FortiManager Administration Guide](#) available on the [Fortinet Document Library](#).

System Settings

This section contains the following topics:

- [Configuring and debugging FortiManager HA clusters on page 14](#)
- [Creating administrator accounts with restricted access on page 16](#)

Configuring and debugging FortiManager HA clusters

You can configure two or more FortiManager units in a high availability (HA) cluster. You can also generate and download a debug log for each unit in a FortiManager HA cluster.

The following is an overview of configuring FortiManager units in an HA cluster:

1. Configure the primary FortiManager unit. See [Configuring the primary FortiManager unit in an HA cluster on page 14](#)
2. Configure one or more backup FortiManager units. See [Configuring backup FortiManager units in an HA cluster on page 15](#)
3. If you encounter problems, review the debug log for each unit in an HA cluster. See [Generating and downloading HA debug logs on page 15](#).

Configuring the primary FortiManager unit in an HA cluster

You can configure one FortiManager unit to be the primary unit in a high availability (HA) cluster. You must know the IP address and serial number of the FortiManager units that will be configured as backup (also called secondary or peer) units in the HA cluster to complete this procedure.

To configure the primary FortiManager unit:

1. Go to *System Settings > HA*.
2. Set *Operation Mode* to *Primary*.
3. In the *Peer IP* box, enter the IP address of the backup FortiManager unit.
4. In the *Peer SN* box, enter the serial number of the backup (secondary or peer) FortiManager unit.

- Click + to add additional backup FortiManager units to the HA cluster.

Cluster Settings

Operation Mode

Standalone

Primary

Secondary

Peer IP and Peer SN

IP Type

Peer IP

Peer SN

IPv4

192.168.48.61

FM200D3A15000236

+

Cluster ID

1

(1-64)

Group Password

File Quota

4096

(2048-20480) MB

Heart Beat Interval

5

Seconds

Failover Threshold

3

(1-255)

Download Debug Log

Download

Apply

- Click *Apply*.

Configuring backup FortiManager units in an HA cluster

You can configure up to four FortiManager units as backup (also called secondary or peer) units in an HA cluster. You must know the IP address and serial number of the primary FortiManager unit in the HA cluster to complete this procedure.

To configure the backup FortiManager unit:

- Go to *System Settings > HA*.
- Beside *Operation Mode*, select *Secondary*.
- In the *Peer IP* box, enter the IP address of the primary FortiManager unit.
- In the *Peer SN* box, enter the serial number of the primary FortiManager unit.
- Click *Apply*.

Generating and downloading HA debug logs

You can run a command to generate a debug log for each FortiManager unit in an HA cluster, and then you can download the logs using the GUI.

To generate a debug log:

- On the primary or backup (secondary) FortiManager unit in an HA cluster, enter the following command:
`diagnose debug application ha 255`

To download a debug log:

- Go to *System Settings > HA*.
- Next to *Download Debug Log*, click *Download*.
- Save the log file (`ha-<date>.log`) to your local computer. It can be opened in a text editor.

Creating administrator accounts with restricted access

When you create an administrator account in FortiManager, by default the account grants access to all ADOMs and all policy packages. However, you can configure administrator accounts with restricted access to the following items:

- ADOMs - see [Restricting administrator access to ADOMs on page 16](#)
- Device groups - see [Restricting administrator access to device groups on page 18](#)
- Policy packages - see [Restricting administrator access to policy packages on page 19](#)

Restricting administrator access to ADOMs


When you create an administrator account, you can specify which ADOMs that users of the account can access. This topic describes the different methods you can use to restrict access.

To create an administrator account and specify ADOM access:

1. Go to *System Settings > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *Specify*, and then select the ADOMs that the administrator account can access.

Create New Administrator

User Name: ADOM-admin

Avatar:  +Add Photo -Remove Photo

Description:

Admin Type: LOCAL

New Password:

Confirm Password:

Admin Profile: Restricted_User

Administrative Domain: All ADOMs All ADOMs except specified

Policy Package Access: All Packages Specify

JSON API Access: None

Theme Mode: Use Global Theme Use Own Theme

Trusted Hosts:

OK

Select Entries (Total: 20)

- ☐ Chassis
- ☐ FortiAnalyzer
- ☐ FortiAuthenticator
- ☐ FortiCache
- ☐ FortiCarrier
- ☐ FortiClient
- ☐ FortiDDoS
- ☐ FortiDeceptor
- ☐ FortiFirewall
- ☐ FortiMail
- ☐ FortiManager
- ☐ FortiNAC

OK Cancel

For example, select only the *root* and 56 ADOMs.

Create New Administrator

User Name

ADOM-admin

Avatar

A

+ Add Photo

- Remove Photo

Description

Admin Type

LOCAL

New Password

Confirm Password

Admin Profile

Restricted_User

Administrative Domain

All ADOMs

All ADOMs except specified ones

Specify

root

56

2 Entries Selected

Policy Package Access

All Packages

Specify

JSON API Access

None

OK

Cancel

4. Set the remaining options, and click **OK**.

When the administrator logs in to FortiManager, they can only access the specified ADOMs. In this example, the specified ADOMs are *root* and *56*.

Select an ADOM

root (5)

FortiGate 7.0

56

FortiGate 7.0

To create an administrator account and exclude access to specific ADOMs:

1. Go to *System Settings > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *All ADOMs except specified ones*, and then select the ADOMs that you do not want the administrator account to access.
In this example, the *root* and *56* ADOMs are excluded from access.

Edit Administrator

User Name

ADOM-admin

Avatar

A

+ Add Photo

- Remove Photo

Description

Admin Type

LOCAL

Admin Profile

Restricted_User

Administrative Domain

All ADOMs

All ADOMs except specified ones

Specify

root

56

2 Entries Selected

Policy Package Access

All Packages

Specify

JSON API Access

None

Theme Mode

Use Global Theme

Use Own Theme

Trusted Hosts

OK

Cancel

4. Set the remaining options, and click **OK**.

When the administrator logs in to FortiManager, they can access all ADOMs except for the ones specified. In this example, they can access all ADOMs except *root* and *56*.

Select an ADOM

Production

Test

FortiGate 6.4

FortiGate 7.0

Restricting administrator access to device groups

On the *Device Manager* pane, you can create device groups and add devices to the different groups. If you are using ADOMs, select the ADOM, and then create the device group.

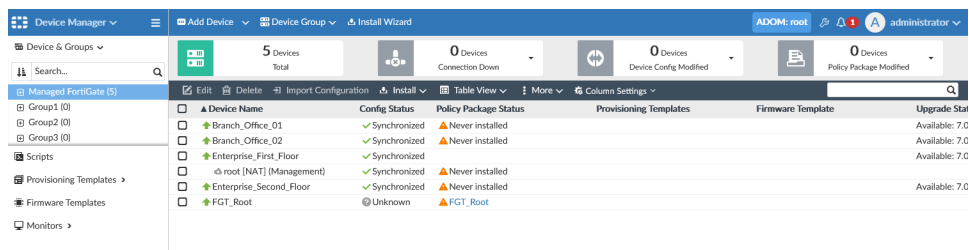
When you create an administrator account, you can specify which ADOMs the account can access, and which device groups can be accessed in those ADOMs.

This topic describes how to create a device group and how to restrict administrator access to device groups.

To create a device group:

1. Go to *Device Manager > Device & Groups*.
2. If you are using ADOMs, select the ADOM that you are creating a device group in. Otherwise skip this step.
3. In the *Device Group* dropdown menu, click *Create New Group*.
4. Enter a name for the group and add devices to it, then click **OK**.

In this example, the root ADOM contains *group1*, *group2*, and *group3*.



To specify admin access to device groups:

1. Go to *System Settings > Administrators*.
2. Click *Create New*.
3. Beside *Administrative Domain*, click *Specify*.
4. Select the ADOM that contains the device group. Select only one ADOM.
5. Select *Specify Device Group to Access*, and then select the device group.
In this example, *group1* is specified.

Create New Administrator

User Name: Devicegrp-admin

Avatar: [Add Photo] [Remove Photo]

Description:

Admin Type: LOCAL

New Password:

Confirm Password:

Admin Profile: Restricted_User

Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify

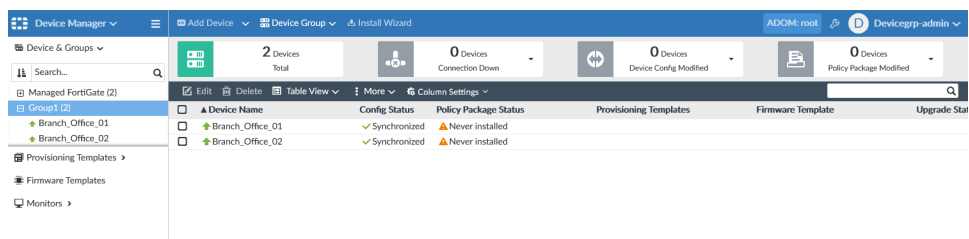
Specify Device Group to Access: ☒ Group1

Policy Package Access: All Packages | Specify

OK Cancel

6. Click *OK*.

When the administrator logs in to FortiManager, they can only access the specified device group on the *Device Manager* pane. In this example, they can only access *group1*.



Restricting administrator access to policy packages


When you create an administrator account, you can specify which policy packages that administrator can access.

To specify admin access to policy packages:

1. Go to *System Settings > Administrators*.
2. Click *Create New*.

3. Beside *Policy Package Access*, click *Specify*, and specify which policy packages can be accessed. In the following example, administrators can access the *root* and *60* policy packages.

New Administrator

User Name	<input type="text" value="Package-admin"/>
Avatar	 <input type="button" value="+ Change Photo"/> <input type="button" value="- Remove Photo"/>
Comments	<input type="text" value=""/> 0/127
Admin Type	<input type="text" value="LOCAL"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
Admin Profile	<input type="text" value="Restricted_User"/>
Administrative Domain	<input type="button" value="All ADOMs"/> <input type="button" value="All ADOMs except specified ones"/> <input type="button" value="Specify"/>
Policy Package Access	<input type="button" value="All Packages"/> <input type="button" value="Specify"/> <input type="text" value="✖ root:default"/> <input type="text" value="✖ 60:default"/>
Trusted Hosts	<input type="button" value="OFF"/>
Meta Fields	>

4. Set the remaining options, and click *OK*.
When the administrator logs in to FortiManager, they can only access the specified policy packages. In this example, the specified policy packages are *root:default* and *60:default*.

Others

This section contains the following topics:

- [Managing FortiAnalyzer from FortiManager on page 21](#)
- [Creating a third party blocklist provider workflow on page 29](#)

Managing FortiAnalyzer from FortiManager

This section contains the following topics:

- [Adding FortiAnalyzer to FortiManager on page 21](#)
- [Viewing managed FortiAnalyzer behavior on page 25](#)
- [Centrally configuring FortiGate to send logs to managed FortiAnalyzer on page 26](#)
- [Viewing logs and reports for managed FortiAnalyzer units on page 26](#)
- [Managing multiple FortiAnalyzer units on page 27](#)
- [Troubleshooting managed FortiAnalyzer units on page 28](#)

Adding FortiAnalyzer to FortiManager

You can add a FortiAnalyzer unit to FortiManager and use FortiManager to manage FortiAnalyzer, but you must add the FortiAnalyzer unit to an ADOM used for central management, which is similar to adding FortiGate units to FortiManager for central management.

You can use the following methods to add FortiAnalyzer units to FortiManager:

- In FortiManager, use the *Add FortiAnalyzer* wizard in the *Device Manager* pane.
- In FortiAnalyzer, enable central management, and then go to FortiManager to authorize the device for central management.

This topic includes the following sections:

- [Preparing to add FortiAnalyzer to FortiManager on page 21](#)
- [Using the wizard to add FortiAnalyzer to FortiManager on page 22](#)
- [Additional information on page 23](#)

Preparing to add FortiAnalyzer to FortiManager

When using FortiManager to manage FortiAnalyzer, it is recommended to use a FortiAnalyzer unit with factory settings or a FortiAnalyzer unit that has been reset to the factory settings (`factory-reset`). A FortiAnalyzer unit with factory settings helps avoid conflicts when FortiManager synchronizes the device database to FortiAnalyzer.

To prepare FortiAnalyzer for management by FortiManager:

1. On the FortiAnalyzer unit, enable fgfm access on the interface used to connect to FortiManager.

```
config system interface
edit "port1"
set ip 10.3.121.142 255.255.0.0
set allowaccess fgfm
next
end
```
2. Create an ADOM with the same name as the ADOM in FortiManager, such as *manage_remote_faz*.
FortiAnalyzer and FortiManager must have an ADOM of the same name. When you add FortiAnalyzer to FortiManager, add it to the ADOM of the same name.
3. Set storage settings for the ADOM.

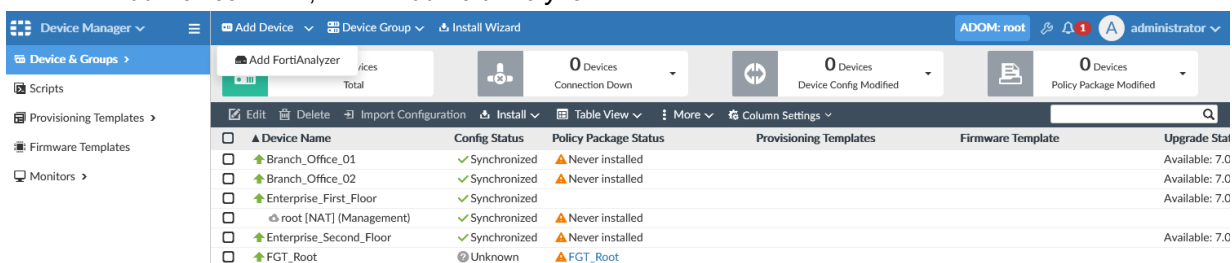
Using the wizard to add FortiAnalyzer to FortiManager

This section describes how to use the *Add FortiAnalyzer* wizard to add FortiAnalyzer to FortiManager.

To add FortiAnalyzer to FortiManager:

1. On FortiManager, ensure that FortiAnalyzer Features are disabled.
 - a. Go to *System Settings > Dashboard*.
 - b. In the *System Information* widget, ensure that *FortiAnalyzer Features* are toggled *Off*.
2. Ensure that the ADOM mode is set to normal by using the following CLI command:

```
config system global
set adom-mode normal
end
```
3. Go to *Device Manager*, and select a central management ADOM, such as *manage_remote_faz*.
The FortiAnalyzer unit should contain an ADOM of the same name. In this example, both FortiAnalyzer and FortiManager have an ADOM named *manage_remote_faz*.
4. On the *Device & Groups* tab, add the FortiAnalyzer unit.
 - a. From the *Add Device* menu, select *Add FortiAnalyzer*.



The *Add FortiAnalyzer* wizard is displayed.

- b. Type the FortiAnalyzer IP address, username, password, and click *Next*.

After FortiManager discovers the device, device information is displayed.

Add FortiAnalyzer

The following information has been discovered from the device:

IP Address	10.3.121.142
Host Name	FAZ1000E
SN	FC18E2B1A000004
Model	FortiAnalyzer-1000E
Firmware Version	6.0.4 build2792 (GA)
HA Status	Standalone
Administrator	Pat

Please input the following information to complete addition of the device:

Name:

Description:

- c. Click **Next** to continue.

Add FortiAnalyzer

Status: Comparing ADOM and devices on both sides...

FortiManager automatically compares ADOMs and devices on both FortiAnalyzer and FortiManager and provides the comparison and verification results.

Add FortiAnalyzer

Status: Verifying managed/logging devices on both sides...

Status	Device Name	Platform
FortiManager Only	FGVMD20000008807	FortiGate-VN64
FortiManager Only	FGVMD20000008808	FortiGate-VN64
FortiManager Only	EQH	FortiGate-VN64
FortiManager Only	Central	FortiGate-VN64
FortiManager Only	NAM	FortiGate-VN64
FortiManager Only	FGVMD20101000073	FortiGate-VN64

- d. Click **Synchronize ADOM and Devices** to continue.

Devices are synchronized between FortiAnalyzer and FortiManager, and FortiAnalyzer is added to FortiManager. The synchronized devices are added to FortiAnalyzer as logging-mode FortiGates.

Add FortiAnalyzer

Status: FortiAnalyzer Added Successfully

FortiAnalyzer is added to FortiManager.

- e. Click **Finish**.

5. Go to **Device Manager > Device & Groups** to view FortiAnalyzer in the *Managed FortiAnalyzer* group.

Device Name	IP Address	Platform	Description
FAZ1000E	10.3.121.142	FortiAnalyzer-1000E	

Additional information

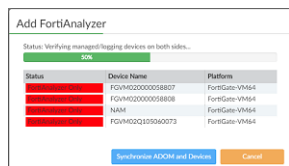
This section describes some of the other scenarios you might encounter when adding FortiAnalyzer units to FortiManager.

Missing ADOM

If the current ADOM in FortiManager does not exist on FortiAnalyzer, FortiManager automatically creates an ADOM with same name and version on FortiAnalyzer before starting to synchronize the device list.

Unknown or mismatched FortiGate devices

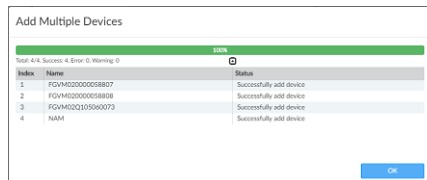
If FortiAnalyzer is receiving logs from FortiGate devices that do not exist on FortiManager, FortiManager identifies the devices.



FortiManager automatically attempts to discover the FortiGates.

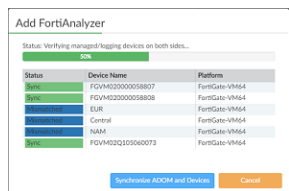


FortiManager can add the FortiGates and retrieve configurations for the FortiGates when adding the FortiAnalyzer unit.

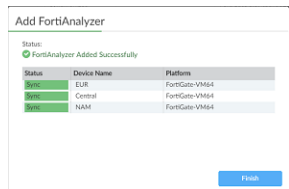


If one device fails to add or retrieve, FortiManager fails to add FortiAnalyzer.

If the same FortiGate device exists on both FortiManager and FortiAnalyzer, but with differences, FortiManager considers the device to be *Mismatched*.



FortiManager tries to synchronize the device settings to FortiAnalyzer.



If any errors occur during the synchronization step, FortiManager fails to add FortiAnalyzer.

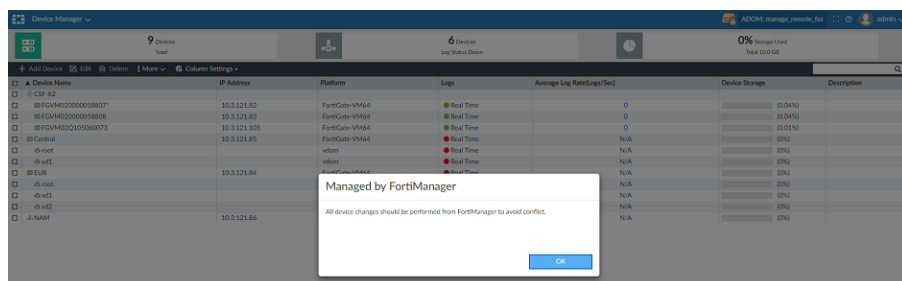
Viewing managed FortiAnalyzer behavior

After FortiManager manages the ADOM with FortiAnalyzer in it, you should use FortiManager to perform changes on all devices in the ADOM. This topic describes the behavior you will view in the GUI for a FortiAnalyzer unit that is managed by FortiManager.

To view managed FortiAnalyzer behavior:

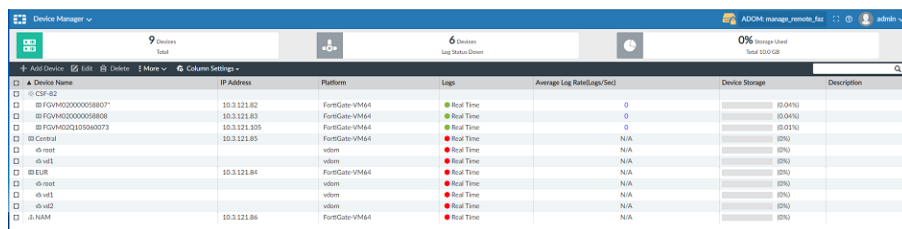
1. Log in to the FortiAnalyzer unit.
2. Go to the *Device Manager* pane.

The *Managed by FortiManager* message is displayed.



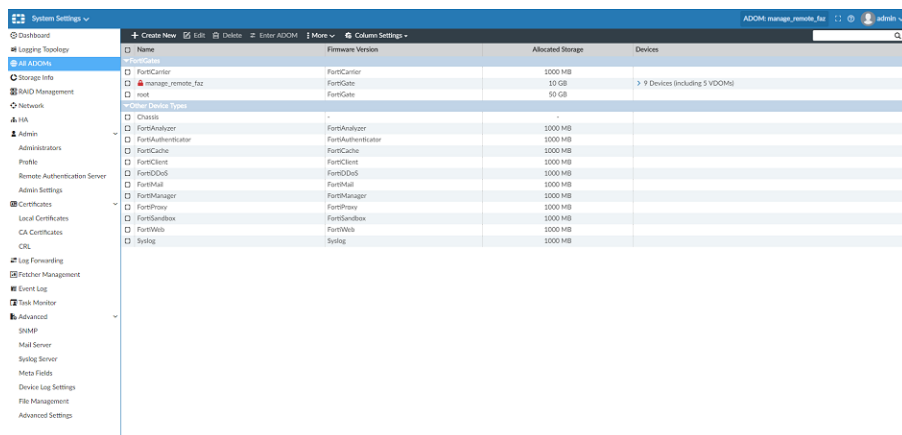
3. Click **OK**.

Notice the *Lock* icon displayed on top bar, and notice that the *Add Device*, *Edit*, and *Delete* buttons are unavailable.



4. Go to *System Settings > All ADOMs*.

Notice the lock icon beside the ADOM that is managed by FortiManager. You can no longer edit devices in the ADOM.

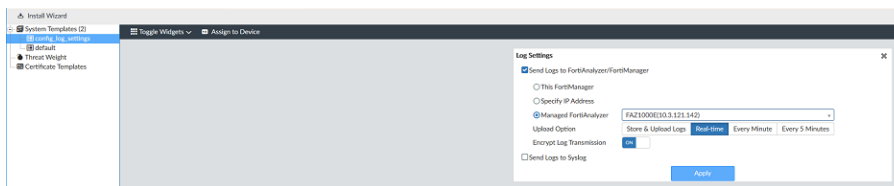


Centrally configuring FortiGate to send logs to managed FortiAnalyzer

After adding FortiAnalyzer to FortiManager, the device list is also synchronized to FortiAnalyzer. To make these FortiGate devices send log to FortiAnalyzer, you can use provisioning templates to centrally configure the log settings for FortiGates.

To centrally configure logging:

1. In FortiManager, go to *Device Manager > Provisioning templates*.
2. Create a new blank system template.
 - a. In the content pane, click *Create New*.
 - b. Type a name for the system template, and click *OK*.
The system template is created.
 - c. Select the system template, and click *Edit*.
The template opens for editing. You can enable the *Log Settings* widget by selecting it from the *Toggle Widgets* dropdown.
- d. In the *Log Settings* widget, select *Send Logs to FortiAnalyzer/FortiManager*.
- e. Select *Managed FortiAnalyzer*, and select the unit from the drop-down list.
- f. Click *Apply*.
3. Assign the system template to FortiGates.
4. Install the system template to FortiGates.



Viewing logs and reports for managed FortiAnalyzer units

After you add FortiAnalyzer to the ADOM in FortiManager, the following FortiAnalyzer panes are available in FortiManager:

- FortiView
- Log View
- FortiSoC
- Reports

All FortiAnalyzer functionality is available, except for the following:

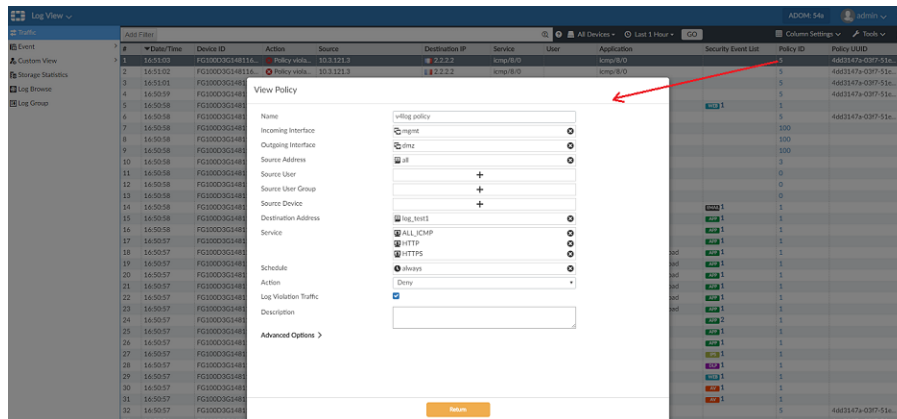
- Importing and exporting a report template
- Importing and exporting a chart
- Importing and downloading a log file

In FortiManager, when you create a report and run it, and the same report is generated in the managed FortiAnalyzer.

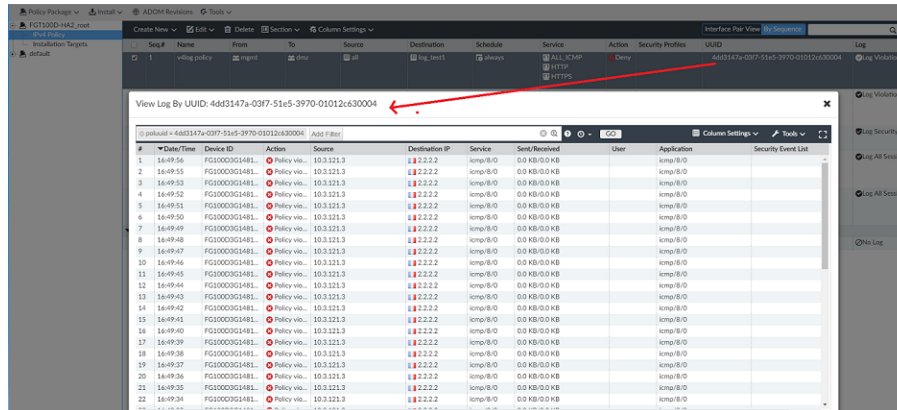
To view logs and reports:

1. On FortiManager, go to **Log View**.
You can view all logs received and stored on FortiAnalyzer.
2. Click the **Policy ID**.
The policy rule opens.

If the policy rule doesn't open, ensure that you have imported the policy rules to the ADOM.



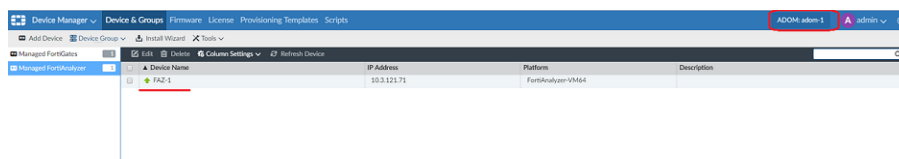
3. Go to **Policy & Objects > Policy Packages**, and right-click the policy UUID to search the related policy logs.



Managing multiple FortiAnalyzer units

FortiManager can manage multiple FortiAnalyzer units, but each FortiAnalyzer must be in its own ADOM. You cannot add a second FortiAnalyzer unit to an ADOM.

For example, FortiManager can contain the following ADOMs: *adom-1* and *adom-2*, and *adom-1* manages FAZ-1:



The other ADOM, *adom-2*, manages FAZ-2:

Device Name	IP Address	Platform	Description
FAZ-2	10.1.1.142	FortiAnalyzer-5000E	

Following is another view of the ADOMs with FortiAnalyzer units:

Name	Firmware Version	Central VPN	Devices
Central Management (5)			
FortiCenter	FortiCenter 5.2		
adom-1	FortiGate 5.4		2 Devices (including 0 VDOMs) • hu-FGT92D • FAZ-2
adom-2	FortiGate 5.4		2 Devices (including 0 VDOMs) • FGVM102000008814 • FAZ-2
root	FortiGate 5.4		
Global Database	Global 5.2		
Other Device Types (11)			
FortiAnalyzer	FortiAnalyzer		
FortiAuthenticator	FortiAuthenticator		
FortiCache	FortiCache		
FortiClient	FortiClient		
FortiCloud	FortiCloud		
FortiMail	FortiMail		
FortiManager	FortiManager		
FortiSandbox	FortiSandbox		
FortiWeb	FortiWeb		
Swing	Swing		
Chassis	.		

Troubleshooting managed FortiAnalyzer units

This topic describes how to troubleshoot several situations.

Adding FortiAnalyzer failed

If adding FortiAnalyzer failed, enable the following debug command, which will provide error or information in a debug log, and then try adding FortiAnalyzer again.

```
diagnose debug application depmanager 255
diagnose debug enable
```

example: add_faz_dep_debug.txt

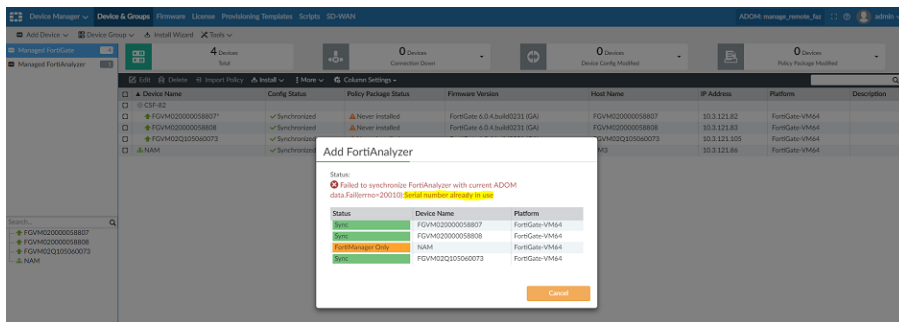
ADOM remains locked on FortiAnalyzer

When you delete FortiAnalyzer from FortiManager, the ADOM on FortiAnalyzer should be unlocked. If the ADOM remains locked, you can use the following command on the FortiAnalyzer unit to unlock the ADOM:

```
FAZ1000E # diag dvm adom unlock
adom ADOM name.
FAZ1000E # diag dvm adom unlock remote-faz
---Deleting DVM lock by remote FortiManager succeeded---
FAZ1000E#
```

Serial number already in use

The Alert console might display the *Serial number already in use* message. FortiManager might also display the *Serial number already in use* message after failing to add FortiAnalyzer.



You can use the `diagnose dvm device list` command on the FortiAnalyzer unit and on the FortiManager unit to see if the same FortiGate unit already exists on the FortiAnalyzer unit, but in different ADOM.

```

FGM000 Login: admin
Password:
FGM000 # diagnose dvm device list
... There are currently 4 device/adoms managed ...

TYPE      QID  SN      HA      IP      NAME      ADOM      IPS      FIRMWARE
mgmt/az enabled 501  FQVM020000058807  10.3.121.82  FQVM020000058807  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; com: up
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/az enabled 513  FQVM020000058808  10.3.121.83  FQVM020000058808  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; com: up
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/az enabled 489  FQVM020105060073  10.3.121.85  FQVM020105060073  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; com: up
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/az enabled 476  FQVM020000058811  10.3.121.86  N/A  root  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; com: up
HA cluster member: FQVM020000058811 (master)
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]

... There are currently 0 FortiAP managed ...

... There are currently 0 FortiSwitch managed ...

... There are currently 0 FortiExtender managed ...

... End device list ...

FGM000 #

FGM1000 Login: admin
Password:
FGM1000 # diagnose dvm device list
... There are currently 4 device/adoms managed ...

TYPE      QID  SN      HA      IP      NAME      ADOM      IPS      FIRMWARE
mgmt/az enabled 273  FQVM020000058807  10.3.121.82  FQVM020000058807  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; com: unknown
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/az enabled 271  FQVM020000058808  10.3.121.83  FQVM020000058808  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; com: unknown
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/az enabled 272  FQVM020105060073  10.3.121.85  FQVM020105060073  manage_remote_faz  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; com: unknown
|- vdom:[1]root flags:0 adom:manage_remote_faz pkg:[never-installed]
mgmt/az enabled 308  FQVM020000058811  10.3.121.86  N/A  root  6.00741 (regular)  6.0 HMD (231)
|- STATUS: dev-db: unknown; conf: unknown; cond: unknown; dm: unknown; com: unknown
HA cluster member: FQVM020000058811 (master)
|- vdom:[1]root flags:0 adom:root pkg:[never-installed]

... There are currently 0 FortiAP managed ...

... There are currently 0 FortiSwitch managed ...

... There are currently 0 FortiExtender managed ...

... End device list ...

FGM1000 #
  
```

Compare the device list on FGM and FAZ. Both FGM and FAZ have device "FQVM020000058811" but it is in different ADOM (on FGM it is in ADOM "manage_remote_faz" on FAZ it is in ADOM "root"). That is why we saw the error "Failed to sync devdb to FAZ: Serial number already in use".

To solve the problem, manually move the device "FQVM020000058811" to ADOM "manage_remote_faz" on FAZ. You may need to rebuild the DB if want to view the old log after move the device.

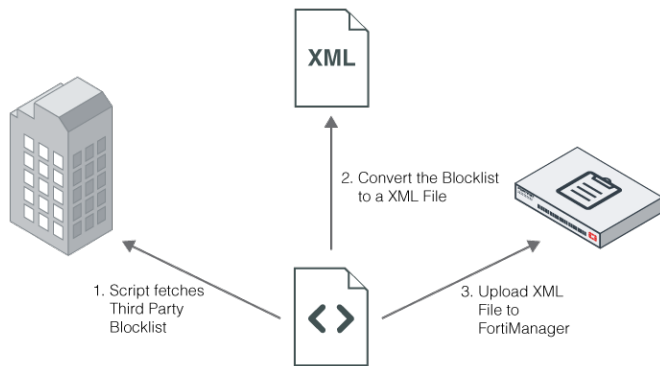
Creating a third party blocklist provider workflow

In this example, you will learn how to use your FortiManager to create a third party blocklist provider workflow.

Overview

You must create a script that will handle the entire workflow. Make sure the script can convert the third party blocklist into a FortiManager XML file.

From an external server, you must schedule the periodic execution of that script. Using the communication tools provided by the third party blocklist provider, the script will fetch the blocklist from the third party.



To create a script to handle a third party blocklist provider workflow:

1. Convert the blocklist to a FortiManager XML file:

The script will convert the blocklist to a FortiManager XML file. This XML file allows you to assign a category to each URL in the list, in addition to a default category. The default category is used as the return value when there is no match.

Example of the FortiManager XML file format:

```
<custom_url_list version="1.0">
<head>
<default_cate>142</default_cate>
<description>the description</description>
</head>
<body>
<url_entry>
<url>http://www.url-0000001.com</url>
<cate>79</cate>
</url_entry>
<url_entry>
<url>http://www.url-0000001.com</url>
<cate>28</cate>
</url_entry>
</body>
</custom_url_list>
```

The category value in `<cate></cate>` could be either a normal web filter category or a local category.

2. Upload the XML file into FortiManager:

The script uses SSH to connect to FortiManager and upload the XML file.

CLI command:

```
execute fmupdate <ftp|scp|tftp> import custom-url <xml filename> <ftp|scp|tftp details>
```

Example:

```
# execute fmupdate scp import custom-url 20M-custom-url.xml 000.000.000.000 00
tmp/FORTIGUARD my_login my_password
```

This operation will replace the current <custom-url> package!

Do you want to continue? (y/n)y

Start getting file from remote SCP Host...

SCP transfer successful.

Packing installation is in process...This could take some time.

lccclient command result:Response=202|

Update successfully

In this example, FortiManager will upload the file from the following file:

```
scp://my_login:my_password@000.000.000.000:00/temp/FORTIGUARD/20M-custom-url.xml
```

3. Configure FortiManager to only use its local FortiGuard database or local blocklist database:

a. Select one of the following:

- Local FortiGuard database
- Local blocklist database
- Or both

```
config fmupdate custom-url-list
  set db_selection <fortiguard-db|custom-url|both>
end
```

4. Test custom URLs managed by FortiManager:

a. Use the CLI in FortiManager to send categorization requests for custom URLs managed by FortiManager.

Example of the CLI command set:

```
# diagnose fmupdate fgd-url-rating FGT SN 1 www.foo.com
url rating flags: 0x2 (2:EXACT_MATCH, 1:PREFIX_MATCH)
rates according to url: 0x37 0x00 0x00 0x00
rates according to ip: 0x00 0x00 0x00 0x00
num_dots:-1, num_slash:-1
database version: 16.45562
0 ms
```

The *FGT SN* can be any FortiGate SN.

The returned category is in a hexadecimal output: *0x37*.

In decimal format, the category is *56* or *Web Hosting*.



The memory capacity of the unit determines the number of URLs FortiManager can manage.

5. Specify FortiManager as the FortiGuard server in FortiGate

a. Go to your FortiGate CLI console and execute the following commands:

```
config system centralmanagement
  set type fortimanager
  set {<IP_address> | <FQDN_address>}
  config serverlist
    edit 1
      set servertype
      update rating
      set serveraddress {<IP_address> | <FQDN_address>}
    next
  end
  set includedefaultservers disable
end
```



For further FortiManager information, refer to the [FortiManager Administration Guides](#) available on the [Fortinet Document Library](#).



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.